## **AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions and listings of claims in the application:

## LISTING OF CLAIMS

- (Currently Amended) A method for managing network resources for externally 1 1. 2 authenticated users, the method comprising: 3 authenticating a user in a first administrative domain; 4 generating a token for the user, the token assigning at least a first role for the user, the 5 first role identifying the user as a member of a pre-defined class of users; and 6 configuring the token to identify the user by the first role to a component of a second 7 administrative domain; and 8 receiving a request from the user to retrieve network resources from the second 9 administrative domain and; 10 determining whether the user is authorized to access the network resources of the second 11 administrative domain based on the first role in the token. 12 1 2. (Original) The method of claim 1, wherein configuring the token to identify the user by 2 the first role includes configuring the token to identify the user as the first role to the 3 component of the second administrative domain without revealing a personal 4 identification of the user to the component. 1 3. (Currently Amended) The method of claim 1, wherein configuring the token to identify 2 the user by the first role includes configuring the token to identify the user by the first 3 role to a policy server external to the first administrative domain, thereby enabling 4 wherein the user is able to retrieve network resources from the second administrative 5 domain according to a policy of the policy server.
- 1 4. (Currently Amended) A method as recited in claim 1,

2		wherein configuring the token to identify the user-by the first role includes configuring
3		the token to identify the user by the first role to a policy server external to the first
4		administrative domain;
5		and further comprising the steps of:
6		receiving a request from the user to retrieve network resources from the second
7		administrative domain;
8		wherein determining whether the user is authorized to access the network resources of the
9		second administrative domain includes determining whether the user is authorized
10		to access the network resources according to a policy of the policy server and
11		based on the first role in the token.
1	5.	(Original) The method of claim 1, wherein generating a token for the user includes
2		assigning multiple roles for the user on the first token, each of the multiple roles being
3		identifiable to a policy server external to the first administrative domain.
1		
1	6.	(Original) The method of claim 1, further comprising the steps of:
2		attaching the token to a terminal associated with the user;
3		automatically receiving the token at the second administrative domain when the user
4		requests one or more resources from the second administrative domain.
1	7.	(Original) The method of claim 1, further comprising the steps of:
2		attaching an indicator for the token to a terminal associated with the user;
3		automatically receiving the indicator to the component to inform the component of a
4		location of the token on another computer.
1	8.	(Original) The method of claim 1, wherein generating a token for the user includes
2		providing information about a quality of authentication for the user.
1	9.	(Original) The method of claim 1, wherein generating a token for the user includes
2		providing information about a location of the user in the token.

1	10.	(Original) The method of claim 1, wherein generating a token for the user includes
2		providing information in the token about a personal identification of the user, a time
3		stamp for when the token was generated, and the first role.
1		
1	11.	(Original) The method of claim 1, wherein generating a token for the user includes
2		providing information in the token selected from a group of information consisting of
3		information about a personal identification of the user, a time stamp for when the token
4		was generated, and the first role; and further including the steps of encrypting at least
5		some of the information in the token for use in the second administrative domain.
1	12.	(Original) A method for managing network resources in multiple administrative domains,
2		the method comprising:
3		in a first administrative domain:
4		authenticating a user in response to a request to access one or more
5		resources in the first administrative domain;
6 .		generating a token for the user, the token assigning at least a first role to
7		the user, the first role identifying the user as a member of a class of users;
8		in second administrative domain:
9		receiving a second request from the user to access one or more second
10		resources in the second administrative domain, wherein the second request
11		includes the token;
12		identifying a first policy for the first role specified by the token; and
13		managing access of the user to the second resources according to the first
14		policy.
1	13.	(Original) The method of claim 12, wherein managing the user according to the first
2		policy includes checking the first policy to determine if an operation requested by the
3		user for the second resources of the second administrative domain is permitted for the
4		first role.
1	14.	(Original) The method of claim 12, wherein managing the user according to the first
2		policy includes checking the first policy to determine if an operation requested by the

user for the second resources of the second administrative domain is permitted for the 3 4 first role. 1 15. (Original) The method of claim 12, wherein managing the user according to the first 2 policy includes checking the first policy to determine if an operation requested by the 3 user for the second resources of the second administrative domain is permitted for the 4 first role, and wherein the method further comprises allowing execution of the operation 5 on the second resources only if the policy permits for the operation to be performed by 6 any user assigned the first role. 1 1 16. (Original) The method of claim 12, wherein managing the user according to the first 2 policy includes checking the first policy to determine if an operation requested by the 3 user for the second resources of the second administrative domain is permitted for the 4 first role, and wherein the method further comprises allowing execution of the operation 5 on the second resources only if the policy permits for the operation to be performed by 6 any user assigned the first role. (Original) The method of claim 12, wherein managing the user according to the first 1 17. 2 policy includes identifying an allowable time period in which any user assigned the first 3 role can access the second resources of the second administrative domain, and wherein 4 the method further includes determining if the user is accessing the second resources of 5 the second administrative domain during the allowable time period 1 18. (Currently Amended ) A method for managing network resources for externally 2 authenticated users, the method comprising: 3 receiving a first request to authenticate a user in a first administrative domain; 4 authenticating [[a]] the user in [[a]] the first administrative domain; 5 generating a token for the user, wherein the token includes information defining a first 6 role for the user, wherein the first role identifies the user as a member of a pre-7 defined class of users; 8 receiving a second request from the user to access one or more network resources located 9 in a second administrative domain; and

10		determining whether to grant the user access to the network resources based on the role in		
11		the token and without re-authenticating the user in the second administrative		
12		domain.		
1	19.	(Cancelled).		
1	20.	(Cancelled)		
1				
1	21.	(Cancelled).		
1	22.	(Cancelled)		
1	23.	(Currently Amended) A computer system for managing network resources, the computer		
2		system comprising:		
3	a storage medium that stores identification information for users that access the network;			
4	processing resources located in a first administrative domain, the processing resources being			
5		configured to:		
6		access the storage medium to identify authenticating a user accessing the network in the		
7		first administrative domain;		
8		generate a token for the user in response to the user accessing the network, the token		
9		identifying at least a first role for the user and identifying the user as a member of		
10		a pre-defined class of users; and		
11		configure the token to enable the user to be identified by the first role in a second		
12		administrative domain, so that wherein the user is provided access to a resource of		
13		the second administrative domain according to a policy for the first role;		
14		receiving a request from the user to retrieve network resources from the second		
15		administrative domain;		
16		determining whether the user is authorized to access the network resources of the second		
17		administrative domain based on the first role in the token.		
18				

1 2 3	24.	(Original) The computer system of claim 23, wherein the processing resource is configured to authenticate the user by accessing the identification information in the first storage medium.
1	25.	(Original) The computer system of claim 23, wherein the processing resources is
2		configured to associate the token with the user for a duration when the terminal of the
3		user is connected to the network.
1		
1	26.	(Original) The computer system of claim 23, wherein the token expires after the terminal
2		is disconnected from the network.
1	27.	(Cancelled)
1	28.	(Cancelled)
1	29.	(Cancelled)
1	30.	(Currently Amended) A computer-readable medium for managing network resources in
2		multiple administrative domains, the computer-readable medium carrying instructions for
3		performing the steps of:
<b>4</b> ·		assigning at least a first role to a plurality of users that access a first administrative
5		domain; and
6		causing each of the plurality of users to be identified by the first role on a component of
7		the second administrative domain, so that wherein the first role identifies a policy
8		that is shared by the plurality of users for accessing resources managed in the
9		second administrative domain.
1		receiving a request from the user to retrieve network resources from the second
2		administrative domain and;
3		determining whether the user is authorized to access the network resources of the second
4		administrative domain based on the first role in the token.
5		

## PRASAD, Ser. No. 09/895,534, GAU 2142, Examiner M. Geckil REPLY TO OFFICE ACTION

- 1 31. (Original) The computer-readable medium of claim 30, further comprising instructions 2 for authenticating the plurality of users in a first administrative domain before assigning 3 at least a first role to the plurality of users.
- 1 32. (Original) The computer-readable medium of claim 30, further comprising assigning at
  2 least the first role to a plurality of users during a network session between each of the
  3 users and the first administrative domain, and causing each of the plurality of users to be
  4 identified by the first role after each of the plurality of users selects to access the second
  5 administrative domain during the network session.
- 1 33. (Original) The computer-readable medium of claim 30, further comprising assigning at
  2 least a first role to a plurality of users includes generating a token that identifies the first
  3 role to a policy server of the second administrative domain.
- 1 34. (Cancelled)